

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-165081  
(P2002-165081A)

(43) 公開日 平成14年6月7日(2002.6.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード(参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 5 7
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	5 0 0 B 5 C 0 6 3
G 0 9 C 5/00		G 0 9 C 5/00	5 C 0 7 6
G 1 0 K 15/02		G 1 0 K 15/02	5 J 1 0 4
H 0 4 N 7/08		H 0 4 N 7/08	Z

審査請求 未請求 請求項の数30 O L (全 26 頁) 最終頁に続く

(21) 出願番号 特願2000-361433(P2000-361433)

(22) 出願日 平成12年11月28日(2000.11.28)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 村谷 博文

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B057 AA11 CA16 CA19 CB16 CE08

CH08 DA07 DA13

5C063 AB03 AC01 AC05 CA23 CA36

DA07 DA13 DB09

5C076 AA14 BA07

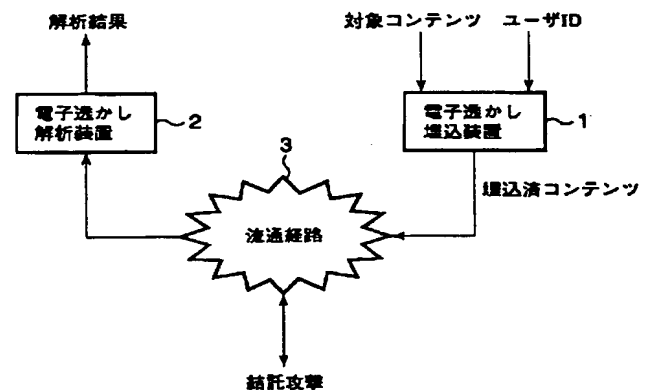
5J104 AA13 AA14

(54) 【発明の名称】 電子透かしシステム、電子透かし解析装置、電子透かし解析方法及び記録媒体

## (57) 【要約】

【課題】 結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステムを提供すること。

【解決手段】 電子透かし埋め込み装置1では、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に、該ユーザのユーザIDに一意に対応する結託耐性符号を埋め込む。コンテンツが流通経路3を経た後に、電子透かし解析装置2では、解析対象となったデジタルコンテンツの複製物から結託耐性符号を検出し、検出された符号を構成する複数の成分符号の各々について改ざん部分の位置に関する位置情報を検出し、該位置情報に基づいて成分符号の改ざん部分の位置に関する所定の統計量を求め、該所定の統計量に基づいて該デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する。



1

## 【特許請求の範囲】

【請求項 1】 結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かしシステムであって、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第 1 のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出し、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求め、求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第 2 のステップとを有することを特徴とする電子透かしシステム。

【請求項 2】 結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステムであって、デジタルコンテンツの複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第 1 のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、

2

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第 2 のステップとを有することを特徴とする電子透かしシステム。

【請求項 3】 結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置であって、解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出する手段と、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出する手段と、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求める手段と、

求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段とを備えたことを特徴とする電子透かし解析装置。

【請求項 4】 前記デジタルコンテンツの複製物は、該複製物がユーザへ渡されるのに先だって、前記複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当てる処理と、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成する処理と、

生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成する処理と、

生成された前記結託耐性符号を埋め込む処理とが行われたものであることを特徴とする請求項 3 に記載の電子透かし解析装置。

【請求項 5】 前記複製物に埋め込まれる前記結託耐性符号を構成する前記複数の成分符号の各々は、連続する所定のビット数の 1 または 0 のみからなるビット列を一単位として、該 1 または 0 のみからなるビット列を、該成分符号に対応する前記整数より 1 減じた個数だけ接続したものであって、かつ、0 のみからなるか、1 のみからなるか、または該成分符号のビット列中において該成分符号に対応する前記整数の値に応じた 1 ヶ所の位置でのみ 0 と 1 が隣接する符号であることを特徴とする請求項 3 または 4 に記載の電子透かし解析装置。

【請求項 6】 前記複製物から検出された前記符号を構成する前記複数の成分符号の各々について、該成分符号を構成する前記所定のビット数を一単位とするビット列に 0 と 1 が混在するものが検出された場合に、該ビット列が結託攻撃によって改ざんされた部分であると判断し、

3

改ざんされたビット列の範囲についての両端部分を特定可能な情報を、前記改ざん部分の位置に係る位置情報として検出することを特徴とする請求項5に記載の電子透かし解析装置。

【請求項7】前記複製物から検出された前記符号を構成する前記複数の成分符号の各々について、改ざんされた部分でないと判断された成分符号については、該成分符号が0のみからなる場合には、該成分符号の全ビット列についての二つの端部のうちの予め定められた一方の端部を、該成分符号が1のみからなる場合には、該成分符号の全ビット列についての二つの端部のうちの予め定められた他方の端部を、該成分符号が連続する複数の0と連続する複数の1とを接続したものである場合には、該連続する複数の0と連続する複数の1との境界部分を、前記改ざん部分の位置に係る位置情報として検出することを特徴とする請求項6に記載の電子透かし解析装置。

【請求項8】検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、

求められた複数の前記最上位ビット側位置をそれぞれ規準化した値に対する第1の平均と、求められた複数の前記最下位ビット側位置をそれぞれ規準化した値に対する第2の平均との一方または両方を求め、

求められた前記第1の平均と前記第2の平均の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項3ないし7のいずれか1項に記載の電子透かし解析装置。

【請求項9】前記所定の関数は、前記複製物に対応するユーザを特定する識別情報に対して所定の方法に従って割り当てられた前記複数の整数の各々についてその値が全識別情報についてランダムに分布すると仮定した場合において、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記第1の平均の値およびまたは前記第2の平均の値との関係に基づくものであることを特徴とする請求項8に記載の電子透かし解析装置。

【請求項10】検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、

求められた複数の前記最上位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第1の比と、求められた複数の前記最下位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット

4

側にあるものの個数についての第2の比との一方または両方を求め、

前記第1の比と前記第2の比の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項3ないし7のいずれか1項に記載の電子透かし解析装置。

【請求項11】前記所定の関数は、前記複製物に対応するユーザを特定する識別情報に対して所定の方法に従って割り当てられた前記複数の整数の各々についてその値が全識別情報についてランダムに分布すると仮定した場合において、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記第1の比の値およびまたは前記第2の比の値との関係に基づくものであることを特徴とする請求項8に記載の電子透かし解析装置。

【請求項12】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置であって、

20 解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出する手段と、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求める手段と、

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類する手段と、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求める手段と、

30 求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段とを備えたことを特徴とする電子透かし解析装置。

【請求項13】前記デジタルコンテンツの複製物は、該複製物がユーザへ渡されるのに先だって、

前記複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当てる処理と、

デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当てる処理と、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成する処理と、

生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成する処理と、

50

5

生成された前記結託耐性符号を埋め込む処理とが行われたものであることを特徴とする請求項 12 に記載の電子透かし解析装置。

【請求項 14】前記弱識別子と前記非弱識別子との分類結果に基づいて、弱識別子に分類された識別子の数と、非弱識別子に分類された識別子の数との比を求め、求められた前記比を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めることを特徴とする請求項 3 ないし 7 のいずれか 1 項に記載の電子透かし解析装置。

【請求項 15】前記所定の関数は、結託攻撃に用いられる複製物の個数を変化させたときに、各々の個数と、その個数について確率的に期待される前記比の値との関係に基づくものであることを特徴とする請求項 14 に記載の電子透かし解析装置。

【請求項 16】前記結託攻撃に用いられた複製物の数の推定値を求める代わりに、前記結託攻撃に用いられた複製物の数の大小レベルを示す情報を求めることを特徴とする請求項 14 に記載の電子透かし解析装置。

【請求項 17】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析方法であって、  
解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出し、  
検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出し、  
前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求め、  
求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定することを特徴とする電子透かし解析方法。

【請求項 18】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析方法であって、  
解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、  
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、  
求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、  
この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、  
求められた前記弱識別子と非弱識別子とに関する所定の

6

統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定することを特徴とする電子透かし解析方法。

【請求項 19】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取り可能な記録媒体であって、  
解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出するための機能と、  
検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出するための機能と、  
前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求めるための機能と、  
求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項 20】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取り可能な記録媒体であって、  
解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出するための機能と、  
検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求めるための機能と、  
求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類するための機能と、  
この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求めるための機能と、  
求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項 21】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムであって、  
解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出するための機能と、  
検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出するための機能と、

7

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求めるための機能と、求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラム。

【請求項 2 2】結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置としてコンピュータを機能させるためのプログラムであって、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出するための機能と、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザーを特定する前記識別子を求めるための機能と、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類するための機能と、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求めるための機能と、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定するための機能とを実現させるためのプログラム。

【請求項 2 3】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第 1 のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第 2 のステップとを有することを特徴とする化学物質透かしシステム。

【請求項 2 4】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子である

8

として誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、

前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、

生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、

10 生成された前記結託耐性符号を前記化学物質製品に埋め込む第 1 のステップと、

解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第 2 のステップとを有することを特徴とする化学物質透かしシステム。

20 【請求項 2 5】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、

対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、

生成された前記結託耐性符号を前記化学物質製品に埋め込む第 1 のステップと、

30 解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出し、

前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求め、

40 求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第 2 のステップとを有することを特徴とする化学物質透かしシステム。

【請求項 2 6】結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、

対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、

50

前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、

割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、

生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、

生成された前記結託耐性符号を前記化学物質製品に埋め込む第1のステップと、

解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、

検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求め、

求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、

この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、

求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数进行推定する第2のステップとを有することを特徴とする化学物質透かしシステム。

【請求項27】前記結託耐性符号の前記化学物質製品への埋め込みは、該化学物質製品の持つ構造のうち透かしの埋め込みに使用される特定部位の構造を当該結託耐性符号の値に基づいて変換することによって行われることを特徴とする請求項23ないし26のいずれか1項に記載の化学物質透かしシステム。

【請求項28】前記化学物質製品が複数の合成材料を合成してなるものである場合に、前記結託耐性符号の該化学物質製品への埋め込みは、個々の合成材料について予め該結託耐性符号の取りうる値の各々に対応させて特定部位の構造を交換させたものを用意しておき、該結託耐性符号の値に基づいて該当する個々の合成材料を選択し、選択した合成材料を合成することによって行われることを特徴とする請求項23ないし26のいずれか1項に記載の化学物質透かしシステム。

【請求項29】前記結託耐性符号の前記化学物質製品からの検出は、該化学物質製品の持つ構造のうち透かしの埋め込みに使用される特定部位の構造を解析することによって行われることを特徴とする請求項23ないし26のいずれか1項に記載の化学物質透かしシステム。

【請求項30】前記化学物質製品の持つアミノ酸の配列構造における特定部位のアミノ酸の置換後の種類によって前記結託耐性符号の内容を表現するようにしたことを特徴とする請求項27ないし29のいずれか1項に記載の化学物質透かしシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステム、電子透かし解析装置及び電子透かし解析方法に関する。

【0002】

【従来の技術】デジタルコンテンツ（例えば、静止画、動画、音声、音楽等）は、多数のデジタルデータで構成された構造を持つ。そして、その構造の中には、データを変更しても、当該デジタルコンテンツの作品の同一性あるいは経済的価値を保持できる部分がある。そのような許容された範囲内のデータを変更することによって、デジタルコンテンツに、種々の情報を埋め込むことができる。このような技術は、電子透かしと呼ばれる。

【0003】電子透かし技術によって、デジタルコンテンツに、様々な透かし情報（例えば、コンテンツの著作権者やユーザの識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を、様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出・利用することができる。

【0004】ここでは、例えば同一のデジタルコンテンツを多数のユーザを対象として配給するときに適用される技術として、デジタルコンテンツの複製物に、当該複製物を個々に識別するための情報（例えば、ユーザIDに一意に対応する透かし情報）を埋め込む場合を考える。

【0005】デジタルコンテンツの複製物に固有の識別情報を埋め込む手法は、そのデジタルコンテンツの複製物が更に複製されて海賊版として出回ったときに、該海賊版から識別情報を検出することによって流出元ユーザを特定することができることから、デジタルコンテンツの違法コピーに対する事前の抑制として機能するとともに、著作権侵害が発生したときの事後の救済にも役立つことになる。

【0006】また、あるユーザがデジタルコンテンツの複製物に埋め込まれた識別情報を無効するためには、ユーザにはどの部分が識別情報を構成するビットであるか分からないので、当該デジタルコンテンツの複製物に相当の改変を加える必要があり、そうすると、当該デジタルコンテンツの経済的価値を損なってしまうので、違法コピーの動機付けを奪うことができる。

【0007】このような状況において違法コピーを可能ならしめる方法として出現したのが、「結託攻撃（collusion attack）」である。

【0008】結託攻撃は、異なる複製物には異なる識別情報が埋め込まれていることを利用するものであり、例えば、複数人で複製物を持ちよって、それらをビット単

11

位で比較することによって、デジタルデータの値が異なる部分を見つけ出し、その部分を改ざん（例えば、多数決、少数決、ランダムイズ等）することによって、識別情報を改ざん、消失させるという方法である（なお、具体的な比較操作は行わず、コンテンツ間で画素値を平均化するなどの操作を行って、同様の結果を得る場合もある）。

【0009】例えば簡単な例で示すと、A氏、B氏、C氏の複製物にそれぞれ、

00...00...

00...11...

11...00...

という識別情報が埋め込まれていた場合に、例えば、

10...01...

という、A氏、B氏、C氏のいずれとも異なる識別情報が埋め込まれたコンテンツを出現させることができてしまう。

【0010】そこで、結託攻撃に対する耐性、すなわち結託攻撃を受けても結託者の全部または一部を特定できるような性質を持つ符号（以下、結託耐性符号と呼ぶ）を電子透かしとして埋め込む方法および該結託耐性符号に基づく追跡アルゴリズム（tracing algorithm；結託攻撃に用いられたコンテンツに埋め込まれた識別番号を特定し、結託者のユーザIDを特定するためのアルゴリズム）が種々提案されている。例えば、その一つにc-secure符号がある（D.Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," CRYPTO' 95, 180-189, 1995.）。

【0011】

【発明が解決しようとする課題】結託攻撃に対する耐性をより強くする、すなわち結託者を特定できなくなる結託数の上限数をより増やすためには、コンテンツに埋め込む符号長をより長くする必要があり、一方、コンテンツに埋め込む符号長にも制限があるので、この種の結託耐性符号およびその結託耐性符号に基づく追跡アルゴリズムでは、符号長を削減するために、結託攻撃に利用された複製物の数に上限を設けている（なお、c-secureのcは、高々c個までの複製物を用いた結託攻撃に対して有効であるという意味である）。もし結託攻撃が許容されている個数を越える数の複製物を用いて行われた場合には、追跡アルゴリズムは、結託攻撃に関与した複製物の識別番号として、誤って、結託攻撃に関与したのではない複製物の識別番号を出力し、結託者でないものが結託者として特定されてしまう、という誤判定が発生することがあり得る。なお、結託攻撃においてそれに関与した複製物以外の複製物の識別番号と同一の識別番号を持つ複製物が生成される可能性と、許容個数以下での誤判定の可能性は、結託耐性符号の設計によって確率的にかなり低く抑えられるので、誤判定は、主に許容個数を越える結託攻撃によって発生する。

12

【0012】しかし、現実には許容個数までの複製物で結託攻撃が行われたか否かは、攻撃者（結託者）のみが知る情報である。攻撃者は、複製物の偽造によって不法に利益を得ることを目的としているため、結託攻撃に用いた複製物の個数を自ら公開することはおよそ考えられない。

【0013】したがって、該結託耐性符号の復号を行う追跡アルゴリズムが結託に関与した複製物の識別番号（あるいは、該識別番号に対応する結託者のユーザID）を出力したとしても、それが、正しく複製物あるいは結託者を特定しているのか、それとも、結託攻撃が許容されている個数を越える数の複製物を用いて行われたために、誤って、結託に使われていなかった複製物あるいはそのユーザを特定してしまったのかを、判別することができない、という問題点がある。

【0014】また、この問題を回避するためには、現実的に結託者が準備することができそうな複製物の個数を想像し、その個数以上の許容個数となるように結託耐性符号を設計するより他なく、どうしても、大きな許容個数を設定することになってしまい、その結果、符号長も大きくなってしまう。

【0015】本発明は、上記事情を考慮してなされたもので、結託耐性符号の埋め込まれたデジタルコンテンツの複製物に対する結託攻撃に用いられたデジタルコンテンツの複製物の数を推定可能な電子透かしシステム、電子透かし解析装置及び電子透かし解析方法を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かしシステムであって、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第1のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出し、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求め、求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第2のステップとを有することを特徴とする。

【0017】また、本発明は、結託攻撃に用いられたデ

13

デジタルコンテンツの複製物の数を推定可能な電子透かしシステムであって、デジタルコンテンツの複製物に対応するユーザを特定する識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた複製物に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、デジタルコンテンツの複製物をユーザへ渡すのに先だって、該複製物に対応するユーザを特定する前記識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記複製物に埋め込む第1のステップと、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求め、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する第2のステップとを有することを特徴とする。

【0018】また、本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置／装置であって、解析対象となったデジタルコンテンツの複製物から、該複製物に結託耐性符号として埋め込まれている符号を検出する手段／ステップと、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出する手段／ステップと、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求める手段／ステップと、求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段／ステップとを備えたことを特徴とする。

【0019】好ましくは、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、求められた複数の前記最上位ビット側位置をそれぞれ規準化した値に対する第1の平均と、求められた複数の前記最下位ビット側位置をそれぞれ規準化した値に対する第2の平均との一方または両方を求め、求められた前記第1の平均と前記第2の平均の一方または両方を、予め定められた所定の関数に入力するこ

14

とによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【0020】また、本発明は、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の最上位ビット側位置と最下位ビット側位置の一方または両方を求め、求められた複数の前記最上位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第1の比と、求められた複数の前記最下位ビット側位置のうち、予め定められた基準位置より上位ビット側にあるものの個数および該基準位置より下位ビット側にあるものの個数についての第2の比との一方または両方を求め、前記第1の比と前記第2の比の一方または両方を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【0021】また、本発明は、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定する電子透かし解析装置／方法であって、解析対象となった前記デジタルコンテンツの複製物から、該複製物に前記結託耐性符号として埋め込まれている符号を検出する手段／ステップと、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた複製物に対応するユーザを特定する前記識別子を求める手段／ステップと、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類する手段／ステップと、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求める手段／ステップと、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記デジタルコンテンツに対する結託攻撃に使用された複製物の数を推定する手段／ステップとを備えたことを特徴とする。

【0022】好ましくは、前記弱識別子と前記非弱識別子との分類結果に基づいて、弱識別子に分類された識別子の数と、非弱識別子に分類された識別子の数との比を求め、求められた前記比を、予め定められた所定の関数に入力することによって、該所定の関数の出力として、結託攻撃に用いられた複製物の数の推定値を求めるようにしてもよい。

【0023】好ましくは、前記結託攻撃に用いられた複製物の数の推定値を求める代わりに、前記結託攻撃に用いられた複製物の数の大小レベルを示す情報を求めるようにしてもよい。

【0024】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り

15

当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第1のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第2のステップとを有することを特徴とする。

【0025】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品を追跡する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第1のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求める第2のステップとを有することを特徴とする。

【0026】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別情報に対して、所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第1のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号を構成する複数の成分符号の各々について、該成分符号の改ざん部分の位置に関する位置情報を検出し、前記複数の成分符号の各々について検出された複数の前記位置情報に基づいて、前記改ざん部分の位置に関する所定の統計量を求め、求められた前記改ざん部分の位置に関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第2のステッ

16

プとを有することを特徴とする。

【0027】化学物質透かしシステム。

【0028】また、本発明は、結託攻撃に用いられた異なる識別情報を透かしとして埋め込まれた同種の化学物質製品の数を推定する化学物質透かしシステムであって、対象となる化学物質製品に埋め込むべき識別子を割り当てる際に、予め定められた非負整数の範囲に属する識別子候補の中から、所定の追跡アルゴリズムによって結託攻撃に用いられた化学物質製品に対応する識別子であるとして誤検出される可能性のより高い弱識別子でないと判断されるものを割り当て、前記化学物質製品に埋め込むべき識別子に対して、該識別子の値に基づく所定の方法に従って、複数の整数を割り当て、割り当てられた前記複数の整数の各々に対応する複数の成分符号を生成し、生成された前記複数の成分符号を接続して埋め込むべき結託耐性符号を生成し、生成された前記結託耐性符号を前記化学物質製品に埋め込む第1のステップと、解析対象となった前記化学物質製品から、該化学物質製品に前記結託耐性符号として埋め込まれている符号を検出し、検出された前記符号に前記所定の追跡アルゴリズムを適用して、結託攻撃に用いられた化学物質製品に対応する前記識別情報を求め、求められた前記識別子を、弱識別子とそれ以外の非弱識別子とに分類し、この弱識別子と非弱識別子との分類結果に基づいて、弱識別子と非弱識別子とに関する所定の統計量を求め、求められた前記弱識別子と非弱識別子とに関する所定の統計量に基づいて、前記化学物質製品に対する結託攻撃に使用された化学物質製品の数を推定する第2のステップとを有することを特徴とする。

【0029】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0030】本発明によれば、結託耐性符号の埋め込まれたデジタルコンテンツの複製物から検出した符号についての統計的な手法に基づく推定（例えば、結託耐性符号における改ざん部分の分布の偏り、あるいは検出された識別子における弱識別子の比率などに関する統計的性質等）に基づく推定）を行うことによって、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定することができる。これによって、追跡アルゴリズムの追跡結果の正誤に関する評価や、結託数自体の情報収集などができるようになる。

【0031】

【発明の実施の形態】 以下、図面を参照しながら発明の

実施の形態を説明する。

【0032】本発明は、同一のデジタルコンテンツの複製物（例えば、静止画、動画、音声、音楽等）の各々に対して、少なくとも、複製物ごとに異なるユーザ識別符号（後述するように、当該複製物に対応するユーザすなわち当該複製物を利用することになるユーザ（例えば、当該複製物を譲渡するユーザ、あるいは当該複製物を貸し渡すユーザ）のユーザ識別子（ユーザID）に一意に対応する識別情報であって結託耐性符号に基づくもの）を透かし情報として埋め込み、検出する場合に適用可能である。

【0033】もちろん、同一のデジタルコンテンツの複製物の各々に対して、さらに、その他の様々な透かし情報（例えば、コンテンツの著作権者の識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出するものであってもよいが、以下では、ユーザ識別符号に関係する部分を中心に説明する（その他の透かし情報を利用する場合における当該その他の透かし情報に関係する部分の構成は特に限定されない）。

【0034】以下で示す構成図は、装置の機能ブロック図としても成立し、また、ソフトウェア（プログラム）の機能モジュール図あるいは手順図としても成立するものである。

【0035】図1に、本発明の実施の形態に係る電子透かし埋込装置と電子透かし解析装置が適用されるシステムの概念図を示す。

【0036】電子透かし埋込装置1と電子透かし解析装置2は、コンテンツ提供側に備えられ、管理される。電子透かし埋込装置1においてデジタルコンテンツに所望の透かしデータを埋め込む方法や、電子透かし解析装置2においてデジタルコンテンツから該透かしデータ自体を取り出す方法は、基本的には任意である（例えば、“松井甲子雄著、「電子透かしの基礎」、森北出版、1998年”等参照）。電子透かし埋込装置1は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。同様に、電子透かし解析装置2は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。また、電子透かし埋込装置1および電子透かし解析装置2をコンテンツ提供側で用いる場合には、それらを一体化して実現することも可能である。

【0037】図2に、電子透かし埋込装置1の構成例を示す。この電子透かし埋込装置1は、ユーザ識別符号として埋め込むべき透かし情報である、ユーザIDに対応する結託耐性符号を生成する符号生成部11と、生成された結託耐性符号（埋め込み符号）を対象コンテンツに埋め込む符号埋込部12とから構成される。

【0038】電子透かし埋込装置1は、対象コンテンツと、これに埋め込むべき対象ユーザのユーザIDとが与えられると、該ユーザIDに対応する結託耐性符号を生成し、ユーザ識別符号として該結託耐性符号が埋め込まれたコンテンツを、該ユーザIDのユーザ向けの複製物として出力する。他の透かし情報を利用する場合には、その際に、必要に応じて他の透かし情報が埋め込まれる。

【0039】電子透かし埋込装置1により得られた各ユーザ向けのコンテンツの複製物は、記憶媒体や通信媒体などを媒介とした流通経路3を経てそれぞれ流通する。複数の複製物を用いた結託攻撃は、この流通経路3にて行われる。

【0040】図3、図4に、電子透かし解析装置2の構成例を示す。

【0041】図3、図4に示されるように、電子透かし解析装置2は、検出対象となるコンテンツからユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）を抽出する符号抽出部21と、検出対象となるコンテンツについて、結託攻撃に使用された複製物の個数を推定する結託数推定部22と、所定の追跡アルゴリズムを実行して、結託攻撃に用いられたであろう複製物の結託耐性符号を特定し、該結託耐性符号に対応するユーザID（ユーザIDが復元できない場合のある追跡アルゴリズムでは、結託攻撃に用いられたであろう結託耐性符号に対応するユーザID、またはユーザIDを復元できなかった旨）を特定する（なお、結託攻撃に用いられたであろう結託耐性符号自体を求めずに、直接、対応するユーザIDを求めるようにしてもよい）追跡アルゴリズム処理部23とを備える。なお、本実施形態では、結託攻撃がなされなかった場合、を、結託攻撃に使用された複製物の個数＝1として扱うものとする。

【0042】ここで、電子透かし解析装置2の結託数推定部22には、（1）結託数推定部22単独で（追跡アルゴリズム処理部23の結果を利用することなしに）、検出対象となるコンテンツから、ユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）を取り出し、取り出したユーザ識別符号を解析することによって、結託攻撃に使用された複製物の個数を推定する形態（結託数推定部の第1の態様）と、（2）追跡アルゴリズム処理部23から出力された追跡結果（例えば結託者の全部または一部のユーザID）に基づいて、結託攻撃に使用された複製物の個数を推定する形態（結託数推定部の第2の態様）とがある。図3は、結託数推定部の第1の態様の場合の構成例であり、図4は、結託数推定部の第1の態様の場合の構成例である。

【0043】結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能であり、特に限定

されない。

【0044】なお、図3や図4において、さらに、結託数推定部22の結果および追跡アルゴリズム処理部23の結果を総合的に判断した判定結果を出力する総合判定部を備えても良い。加工処理部は、例えば、推定結託数が許容数以下で且つ結託者のユーザID（の集合）が得られた場合には、当該結託者のユーザID（の集合）を出力し（または、これに加えて推定結託数を出力し）、推定結託数が許容数を越え且つ結託者のユーザID（の集合）が得られた場合には、推定結託数オーバーによる判定不能である旨（または、これに加えて推定結託数）を出力する。もちろん、その他の総合判定結果の生成の仕方も可能である。

【0045】なお、上記の（1）の場合には、結託数推定部22による処理と、追跡アルゴリズム処理部23による処理は、いずれを先に行ってもよいし、並列的に行ってもよい。

【0046】また、上記の（1）の場合には、結託数推定部22を持ち且つ追跡アルゴリズム処理部23を持たない電子透かし解析装置2もあり得る。図5に、この場合の構成例を示す。

【0047】本実施形態によれば、電子透かし解析装置2は結託数推定部22によって結託攻撃に用いられたであろう複製物の個数を推定することができ、これによって追跡アルゴリズムの追跡結果の正誤に関する評価や、結託数自体の情報収集などができるようになる。

【0048】以下では、電子透かし埋込装置1についてより詳細に説明する。

【0049】図6に、概略的な手順の一例を示す。

【0050】符号生成部11は、まず、対象複製物に、埋め込むべきユーザIDに対応する、M（Mは複数）個の整数A（1）、A（2）、…、A（M）を求める（ステップS1）。該M個の整数は、予め求めて記憶しておく方法と、必要時に求める方法とがある。

【0051】各i（i=1～M）におけるそれぞれの整数A（i）は、0～N（i）-1のいずれかの値を取るものとする。ここで、N（1）、N（2）、…、N（M）は、予め定められた相互に異なる正整数とする。より好ましくは、N（1）、N（2）、…、N（M）は、互いに素である。

【0052】ユーザIDに対応するM個の整数A（i）の各々には、0～N（i）-1の範囲でランダムに値を割り当てる方法と、0～N（i）-1の範囲で一定の規則に従って値を割り当てる方法とがある。また、いずれも場合についても、各ユーザIDには、互いにA

（1）、A（2）、…、A（M-1）のうちの少なくとも\*

A（1）=0のとき	:	W（1）=111 111 111 111
A（1）=1のとき	:	W（1）=000 111 111 111
A（1）=2のとき	:	W（1）=000 000 111 111
A（1）=3のとき	:	W（1）=000 000 000 111

\*も一つが相違するように排他的に割り当てる方法と、A（1）、A（2）、…、A（M）のすべてを同一とするM個の整数の組を複数のユーザIDに重複に割り当てることを許す方法とがある。

【0053】排他的に値を割り当てる方法には、例えば、ユーザIDの値として、0～N（1）×N（2）×…×N（M）-1の範囲の整数の全部または一部を使用するものとし、M個の整数A（i）の各々について、対象ユーザIDをN（i）で割ったときの余りを、該ユーザIDに対応するA（i）の値とする方法がある。

【0054】なお、ユーザIDから、該ユーザIDに対応する整数A（1）、A（2）、…、A（M）の組を算出できない方法を用いる場合には、各ユーザIDと、該ユーザIDに対応する整数A（1）、A（2）、…、A（M）の組との対応関係情報を保存しておく必要がある。また、ユーザIDから、該ユーザIDに対応する整数A（1）、A（2）、…、A（M）の組を算出できる方法を用いる場合には、各ユーザIDと、該対応関係情報を保存せずに必要に応じて再計算するようにしてもよいし、該対応関係情報を保存しておいてこれを参照するようにしてもよい。

【0055】次に、符号生成部11は、対象複製物に埋め込むべきユーザIDに対応する、M個の整数A

（1）、A（2）、…、A（M）から、該ユーザIDに対応する結託耐性符号を生成する（ステップS2）。各ユーザIDに対応する結託耐性符号は、予め生成して記憶しておく方法と、必要時に生成する方法とがある。

【0056】各ユーザIDに対応する結託耐性符号は、該ユーザIDに対応するM個の整数A（1）、A（2）、…、A（M）の各々について、対応する成分符号W（1）、W（2）、…、W（M）を求め、それらを連結することによって生成する。

【0057】整数A（i）に対応する成分符号W（i）としては、例えば、 $\Gamma_0(n, d)$ 符号（1または0のみからなる連続したdビットを一つの単位B（j）とし、B（0）～B（n-2）を連結したもの；ただし、B（0）～B（n-2）は、すべてが0のみからなるか、すべてが1のみからなるか、またはB（0）～B（m）までは0のみからなり且つB（m）～B（n-2）までは1のみからなるものである）を用いることができる。例えば、対象ユーザIDをN（i）で割った余りを該ユーザIDに対応する整数A（i）の値とする方法の場合の簡単な例を示すと、N（1）=5の場合、n=5となり、d=3とすると、 $\Gamma_0(5, 3)$ 符号は、以下のようになる。

A（1）=0のとき	:	W（1）=111 111 111 111
A（1）=1のとき	:	W（1）=000 111 111 111
A（1）=2のとき	:	W（1）=000 000 111 111
A（1）=3のとき	:	W（1）=000 000 000 111

21

$$A(1) = 4 \text{ のとき} : W(1) = 000 \ 000 \ 000 \ 000$$

このようにして求めた各  $A(i)$  に対応する成分符号  $W(i)$  を連結することによって、結託耐性符号を生成することができる。

【0058】この符号では1と0はそれぞれ  $d$  ビットを単位として連続するように配置され、 $d$  ビット未満の数の1や0が孤立して存在することはない（上記の例では、3ビット未満の数の1や0が孤立して存在することはないことがわかる）。したがって、 $d$  ビット未満の数の1や0が孤立して存在する場合には、結託攻撃がなされたことが推定される（ $d$  ビット未満の数の1や0が孤立して存在しない場合には、結託攻撃がなされなかったことが推定される）。

【0059】このようにして生成された結託耐性符号は、電子透かし埋込装置1の符号埋め込み部12によって、対象コンテンツに埋め込まれる（ステップS3）。

【0060】図7に、符号生成部11の一構成例を示す。

【0061】この符号生成部11は、それぞれ  $k'$ （= $M$ ）個の法記憶部121-1, 121-2, ..., 121- $k'$ 、剰余計算部122-1, 122-2, ..., 122- $k'$ 、成分符号生成部124-1, 124-2, ..., 124- $k'$  と、符号パラメータ記憶部123及び符号接続部125からなる。

【0062】法記憶部121-1, 121-2, ..., 121- $k'$  には、互いに素の関係にある整数、この例では相異なる  $k'$  個の素数  $p_i$ （= $N(i)$ ）（ $i=1, 2, \dots, k'$ ）が記憶されており、これらの素数  $p_i$  が剰余計算部122-1, 122-2, ..., 122- $k'$  に法として供給される。剰余計算部122-1, 122-2, ..., 122- $k'$  は、入力されるユーザID= $u$  に対して、素数  $p_i$  を法とする剰余  $u_i = u \bmod p_i$ （ $i=1, 2, \dots, k'$ ）をそれぞれ求める。すなわち、入力されたユーザIDに対応した複数の整数要素の組として、剰余計算部122-1, 122-2, ..., 122- $k'$  により剰余  $u_i = u \bmod p_i$ （ $i=1, 2, \dots, k'$ ）が計算される。なお、この例では、 $p_i$ （ $i=1, 2, \dots, k'$ ）は、素数としたが、互いに素な整数であってもよい。

【0063】成分符号生成部124-1, 124-2, ..., 124- $k'$  は、 $k'$  個の素数  $p_i$ （ $i=1, 2, \dots, k'$ ）に対して、符号パラメータ記憶部23に記憶された符号パラメータ  $t$  に従って剰余計算部122- $i$  \*  

$$A(1) = 7 \bmod N(1) = 0$$

$$A(2) = 7 \bmod N(2) = 0$$

$$A(3) = 7 \bmod N(3) = 0$$

となる。

【0071】図10に、この例においてユーザID=0~14の各々について求められた  $A(1)$ 、 $A(2)$ 、 $A(3)$  を示す。

22

\*1, 122-2, ..., 122- $k'$  により求められた剰余  $u_i$ （ $i=1, 2, \dots, k'$ ）を表す前述した  $\Gamma_0(n, d)$  符号からなる成分符号  $\Gamma_0(p_i, t)$  をそれぞれ生成する。すなわち、成分符号生成部124-1, 124-2, ..., 124- $k'$  では、所定個数( $n$ )のユーザIDに対して剰余計算部122-1, 122-2, ..., 122- $k'$  で計算される全ての剰余  $u_i$ （ $i=1, 2, \dots, k'$ ）の組を表現可能な  $k'$  個の成分符号のうちの  $k$  個の組み合わせがユーザIDを一意に表現できる成分符号  $\Gamma_0(p_i, t)$  を各剰余に対応して生成する。

【0064】符号接続部125は、成分符号生成部124-1, 124-2, ..., 124- $k'$  により生成された各成分符号  $\Gamma_0(p_i, t)$  を連結することによって、透かし情報である結託耐性符号を生成する。

【0065】図8に、成分符号生成部124-1, 124-2, ..., 124- $k'$  の一つ(124- $i$ )の構成を示す。符号パラメータを  $t$ 、剰余を  $u_i$ 、法を  $p_i$  とすると、減算部131では  $p_i - u_i - 1$  が求められる。

“0”列生成部132では、符号パラメータ  $t$  と剰余  $u_i$  に基づき  $t \times u_i$  ビットの連続した“0”列が生成され、“1”列生成部133では、符号パラメータ  $t$  と減算部131からの出力  $p_i - u_i - 1$  に基づき  $t \times (p_i - u_i - 1)$  ビットの連続した“1”列が生成される。そして、これらの“0”列と“1”列が接続部34で接続され、 $t \times (p_i - 1)$  ビットのビット列が  $\Gamma_0(n, d)$  符号からなる成分符号  $\Gamma_0(p_i, t)$  として生成される。

【0066】図9は、こうして生成される結託耐性符号の成分符号(結託攻撃を受ける前の成分符号)の一例を示している。0から  $n-1$  までの  $n$  個のユーザIDに対応して、 $B(0)$ , ...,  $B(n-2)$  のブロック“0”列からなる成分符号が割り当てられている。

【0067】ここで、上記の符号生成方法について数値を小さくとして簡単にした例を用いて説明する。

【0068】まず、整数の個数  $M$  を3とし、 $N(1) = 3$ 、 $N(2) = 5$ 、 $N(3) = 7$  とする。この場合、 $A(1)$  は0~2のいずれか、 $A(2)$  は0~4のいずれか、 $A(3)$  は0~6のいずれかとなる。

【0069】次に、 $N(1) \times N(2) \times N(3) - 1 = 104$  であるので、0~104の範囲の全部または一部をユーザIDとして用いる。ここでは、そのうち0~14をユーザIDとして用いるものとする。

【0070】例えば、ユーザID=7の場合、  
 $\bmod \ 3 = 1$ 、  
 $\bmod \ 5 = 2$ 、  
 $\bmod \ 7 = 0$ 、

【0072】次に、 $\Gamma_0(n, d)$  符号において  $d=3$  とした場合における  $A(1)=0$ 、 $A(1)=1$ 、 $A(1)=2$  のそれぞれに対応する成分符号  $W1$  は、次のようになる（なお、分かりやすくするために、0または

50

23

1を、3ビット単位に分けて記述している)。

A (1) = 0 : W1 = 111 111

A (1) = 1 : W1 = 000 111

A (1) = 2 : W1 = 000 000

A (2) = 0 : W2 = 111 111 111 111

A (2) = 1 : W2 = 000 111 111 111

A (2) = 2 : W2 = 000 000 111 111

A (2) = 3 : W2 = 000 000 000 111

A (2) = 4 : W2 = 000 000 000 000

また、同様に、A (3) = 0、A (3) = 1、A (3) = 2、A (3) = 3、A (3) = 4、A (3) = 5、A (3) = 6のそれぞれに対応する成分符号W3は、次のようになる。

A (3) = 0 : W3 = 111 111 111 111 111 111

A (3) = 1 : W3 = 000 111 111 111 111 111

A (3) = 2 : W3 = 000 000 111 111 111 111

A (3) = 3 : W3 = 000 000 000 111 111 111

A (3) = 4 : W3 = 000 000 000 000 111 111

A (3) = 5 : W3 = 000 000 000 000 000 111

A (3) = 6 : W3 = 000 000 000 000 000 000

したがって、例えば、ユーザID=7の場合、A (1) = 1、A (2) = 2、A (3) = 0であるから、

W1 = 000 111

W2 = 000 000 111 111

W3 = 111 111 111 111 111 111

となり、ユーザID=7に対応する結託耐性符号は、それらを連結して、

000111 000000111111 1111111111111111

となる(なお、分かりやすくするために、W1~W3に対応する部分の境界で分けて記述している)。

【0073】図11に、この例において各ユーザID=0~14について求められた結託耐性符号を示す。

【0074】次に、電子透かし解析装置2についてより詳細に説明する。

【0075】ここで、上記の例を利用して、結託攻撃について説明する。

【0076】例えば、上記のユーザID=2のユーザが入手したコンテンツには、ユーザ識別符号として、

000000 000000111111 0000001111111111

が埋め込まれている(図10、図11参照)。また、例えば、上記のユーザID=3のユーザが入手したコンテンツには、ユーザ識別符号として、

111111 000000000111 0000000001111111

が埋め込まれている(図10、図11参照)。

【0077】この場合に、ユーザID=2のユーザとユーザID=3の2人のユーザが持ちよったコンテンツを比較すると、上記36ビットのうち、左から1~6番目、13~15番目、25~27番目が相違していることがわかる。そこで、それらが識別情報の一部と分かるため、1~6番目、13~15番目、25~27番目のうちの一部に改ざんが施され、例えば、次のような改変が施される。

010101 000000010111 0000001011111111

24

\*また、同様に、A (2) = 0、A (2) = 1、A (2) = 2、A (2) = 3、A (2) = 4のそれぞれに対応する成分符号W2は、次のようになる。

10 ※ (3) = 6のそれぞれに対応する成分符号W2は、次のようになる。

A (3) = 0 : W3 = 111 111 111 111 111 111

A (3) = 1 : W3 = 000 111 111 111 111 111

A (3) = 2 : W3 = 000 000 111 111 111 111

A (3) = 3 : W3 = 000 000 000 111 111 111

A (3) = 4 : W3 = 000 000 000 000 111 111

A (3) = 5 : W3 = 000 000 000 000 000 111

A (3) = 6 : W3 = 000 000 000 000 000 000

★ ★ = 1、A (2) = 2、A (3) = 0であるから、

同様に、ユーザID=7のユーザとユーザID=8との2人のユーザで、例えば、次のような改ざんが施される。

000010 000000101111 0101111111111111

また、同様に、ユーザID=3、4、5、6の4人のユーザによって、例えば、次のような改ざんが施される。

010101 010101010101 000000000010101010

次に、追跡アルゴリズムの概要を説明する。

【0078】符号抽出部21によって、検出対象となるコンテンツからユーザ識別符号(埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの)が抽出されると、追跡アルゴリズム処理部23は、抽出された符号を解析することによって、結託攻撃に用いられたであろう複製物の結託耐性符号を推定し、該結託耐性符号に対応するユーザIDを推定する。

【0079】ここで、図12(a)に示すように、符号(生成された結託耐性符号、結託攻撃を受けた結託耐性符号)の成分符号(上記の例では3つの成分符号)の各々ごとについて、当該成分符号の両端の位置と、隣接する要素B(d-1)とB(d)との境界の位置を、数値化して表すものとする。すなわち、第i番目の成分符号W(i)の要素B(j)の数をN(i)-1個とし、図12(a)でN(i)をNで表すものとする、要素B(0)の左端の位置が0、要素B(d-1)とB(d)との境界の位置がd、要素B(N-2)の右端の位置がN-1で表される。

【0080】そして、コンテンツから検出された符号の第i番目の成分符号W(i)を、左端のビットからみて

50

いったときにはじめて出現する、0のみからなる要素B ( $s-1$ )と1を含む要素B ( $s$ )との境界を求め、該境界に対応する上記の位置を示す値  $s$  を、 $Amin(i)$  で表すものとする。一方、右端のビットからみていったときにはじめて出現する、1のみからなる要素B ( $t$ )と0を含む要素B ( $t-1$ )との境界を求め、該境界に対応する上記の位置を示す値  $t$  を、 $Amax(i)$  で表すものとする。

【0081】例えば、図12(b)の符号の例では、 $Amin(i)=2$ 、 $Amax(i)=4$ となる。また、例えば、図12(c)の符号の例では、 $Amin(i)=2$ 、 $Amax(i)=2$ となる。また、例えば、図12(d)の符号の例では、 $Amin(i)=4$ 、 $Amax(i)=4$ となる。なお、第  $i$  番目の成分符号  $W(i)$  が0のみからなる場合には、 $Amin(i)=Amax(i)=N(i)-1$ となる。また、1のみからなる場合には、 $Amin(i)=Amax(i)=0$ と\*

A(3)=0: W3=111 111 111 111 111 111  
 A(3)=1: W3=000 111 111 111 111 111  
 A(3)=2: W3=000 000 111 111 111 111  
 A(3)=3: W3=000 000 000 111 111 111  
 A(3)=4: W3=000 000 000 000 111 111  
 A(3)=5: W3=000 000 000 000 000 111  
 A(3)=6: W3=000 000 000 000 000 000

を比較して分かるように、その性質上、複数の複製物から得られる相違部分は、必ず連続した要素Bとして得られることがわかる(したがって、結託攻撃による改ざんによって、この連続した部分に0と1が混在してくることになる)。

【0084】そして、ある成分符号( $i$ )において、その  $d$  ビット未満の数の1や0が孤立して存在する連続した部分の左端の位置と右端の位置、すなわち  $Amin(i)$  と  $Amax(i)$  は、必ず、結託攻撃に用いられた複数の複製物のいずれかに埋め込まれた結託耐性符号の対応する成分符号の0と1の区切り目の位置(成分符号がすべて1の場合は、該成分符号の左端の位置、すべて0の場合は、該成分符号の右端の位置)すなわち  $Amin(i)=Amax(i)$  に一致することがわかる。このような情報が、各成分符号  $W(i)$  毎に得られる。それら情報  $Amin(1)$ 、 $Amin(2)$ 、…、 $Amin(M)$ 、 $Amax(1)$ 、 $Amax(2)$ 、…、 $Amax(M)$  を解析することによって、結託攻撃に使用された複製物に埋め込まれていたであろうユーザ識別符号すなわち結託耐性符号を特定し、該結託耐性符号に対応するユーザIDを、結託攻撃を行った結託者のユーザIDとして特定することができる。

【0085】簡単な例としては、2人のユーザによる結託攻撃では、各成分符号ごとにおいて、 $Amin(i)$  は、2人のユーザの一方の持つ複製物に埋め込まれた符号の  $Amin(i)=Amax(i)$  に一致し、 $Ama$

\*なる。

【0082】さて、追跡アルゴリズムでは、検出された符号の各々の成分符号を調べ、予め定められた  $d$  (上記の例の場合、3) ビット未満の数の1や0が孤立して存在する成分符号が検出された場合に、結託攻撃がなされたものと判断することができる。また、この場合に、結託数が予め規定された許容数以下であったものと仮定して、上記の各々の成分符号  $W(i)$  の第1の境界あるいは境界の最小値  $Amin(i)$  や第2の境界あるいは境界の最大値  $Amax(i)$  に基づいて、結託攻撃に使用された複製物に埋め込まれていたであろう結託耐性符号を推定することができる。そして、結託耐性符号から、対応するユーザIDを求め、これを結託攻撃を行った結託者のユーザIDとして特定することができる。

【0083】各々の  $A(i)$  に対応する成分符号  $M(i)$  は、例えば、先に例示したもの、すなわち、

$x(i)$  は、他方のユーザの持つ複製物に埋め込まれた符号の  $Amin(i)=Amax(i)$  に一致する(各成分符号ごとに一方と他方の対応は異なりうる)。  $Amin(1)$  と  $Amax(1)$  からいずれか1つ、  $Amin(2)$  と  $Amax(2)$  からいずれか1つ、…  $Amin(M)$  と  $Amax(M)$  からいずれか1つを選択したものを、それぞれ、各成分符号の0と1の区切り目の位置として持つような結託耐性符号が存在すれば、それが求める解であり、該結託耐性符号に対応するユーザIDが結託者を示すことになる。

【0086】例えば、先の図10、図11の例で示したように、ユーザID=2のユーザが入手したコンテンツに、ユーザ識別符号として、

000000 000000111111 0000001111111111

が埋め込まれており、ユーザID=3のユーザが入手したコンテンツに、ユーザ識別符号として、

111111 000000000111 0000000001111111

が埋め込まれており、当該2人のユーザによって結託攻撃がなされ、次のようなユーザ識別符号、

010101 000000010111 0000001011111111

に改ざんされた場合に、この改ざん符号では、

$Amin(1)=0$ 、 $Amax(1)=2$

$Amin(2)=2$ 、 $Amax(1)=3$

$Amin(1)=2$ 、 $Amax(1)=3$

であり、図10あるいは図12を参照すると、 $Amin(1)=2$ 、 $Amax(1)=2$ 、 $Amax(1)=2$

10

30

40

50

27

を、ユーザID=2が満たし、かつ、 $A_{min}(1) = 0$ 、 $A_{max}(1) = 3$ 、 $A_{max}(1) = 3$ を、ユーザID=3が満たすので、この結託攻撃は、ユーザID=2とユーザID=3によって行われ、結託攻撃に用いられた符号は、

000000 000000111111 000000111111111111

と、

111111 000000000111 000000000111111111

であることを突き止めることができる。

【0087】なお、3人以上のユーザによる結託攻撃では、これに用いられた全複製物に埋め込まれた結託耐性符号（ユーザ識別符号）の全成分符号が本来持つ $A_{min}(i) = A_{max}(i)$ の全ては得られないことがあるが、ある複製物に埋め込まれた結託耐性符号の全てであるいはそのうちの多数の成分符号について $A_{min}(i) = A_{max}(i)$ が得られたことが期待されるので、対象コンテンツから検出された符号から得られた $A_{min}(1)$ 、 $A_{min}(2)$ 、…、 $A_{min}(M)$ 、 $A_{max}(1)$ 、 $A_{max}(2)$ 、…、 $A_{max}(M)$ を適宜組み合わせることで検証することによって、かりにすべての結託者のユーザIDが特定できなかったとしても、一部の結託者のユーザIDを特定することができる。

【0088】さて、符号抽出部21によって、検出対象となるコンテンツからユーザ識別符号（埋め込まれた結託耐性符号または結託攻撃が施されて改ざんされたもの）が抽出されると、電子透かし解析装置2の結託数推定部22は、抽出された符号を解析することによって、結託攻撃に用いられたであろう複製物の結託数を推定する。

【0089】以下では、電子透かし解析装置2の結託数推定部22について説明する。

【0090】（第1の構成例）まず、図3や図5に例示されるような、結託数推定部22単独で（追跡アルゴリズム処理部23の結果を利用することなしに）、結託攻撃に使用された複製物の個数を推定する場合（結託数推定部の第1の態様の場合）について説明する。なお、前述したように、結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能である。また、結託攻撃がなされなかった場合を、結託攻撃に使用された複製物の個数=1として扱うものとする。

【0091】図13に、この場合の結託数推定部22の構成例を示す。図13に示されるように、この結託数推定部22は、抽出された符号（ユーザ識別符号）の各々の成分符号 $W(1)$ 、 $W(2)$ 、…、 $W(M)$ から、先に説明した、 $A_{min}(1)$ 、 $A_{min}(2)$ 、…、 $A_{min}(M)$ のM個の第1グループのデータと、 $A_{max}(1)$ 、 $A_{max}(2)$ 、…、 $A_{max}(M)$ のM個の第2グループのデータ的一方または両方を求める境界検出部221、求められた第1グループのデータと第2

28

グループのデータ的一方または両方から統計的な量を求める統計処理部222、求められた統計的な量から結託数の推定値C0を求める推定結託数算出部223を含む。

【0092】図14に、概略的な手順の一例を示す。

【0093】ここで、図15に、結託攻撃において用いた複製物の個数（図15ではcと表す）を変えたときに、それに対応して、改ざん後の符号の各成分符号 $W(i)$ から検出される第1の境界 $A_{min}(i)$ がどのような値をとるか、その確率を表す。なお、図15では、 $A_{min}(i)$ が取りうる最大値（ $=N(i)-1$ ）と最小値（ $=0$ ）との差（ $=N(i)$ の値）で除して正規化する。また、第1の境界 $A_{max}(i)$ については、 $A_{min}(i) = 1 - A_{max}(i)$ の関係になる（図15の横軸の0を1.0に、1.0を0に入れ替えたものになる）。

【0094】これより分かるのは、第1の境界 $A_{min}$ については、結託数cが大きくなると、 $A_{min}$ が小さな値をとる確率がより大きくなるように、バイアスされてくるということである。同様に、第2の境界 $A_{max}$ については、cが大きくなると、 $A_{max}$ が大きな値をとる確率がより大きくなるように、バイアスされてくるということである。

【0095】したがって、複数の $W(i)$ に対して、M個の $A_{min}(i)$ （または $A_{max}(i)$ ）の値をもとめ、それらM個の $A_{min}(i)$ （または $A_{max}(i)$ ）の分布を解析することによって、結託数cの値を統計的に推定することができることになる。

【0096】統計処理部222および推定結託数算出部223による統計的な処理の方法には種々のバリエーションが考えられる。以下では、2つのバリエーションを説明する。

【0097】（バリエーション1）まず、境界検出部221は、抽出された符号の各々の成分符号 $W(1)$ 、 $W(2)$ 、…、 $W(M)$ から、先に説明した、 $A_{min}(1)$ 、 $A_{min}(2)$ 、…、 $A_{min}(M)$ のM個の第1グループのデータと、 $A_{max}(1)$ 、 $A_{max}(2)$ 、…、 $A_{max}(M)$ のM個の第2グループのデータ的一方または両方を求める（ステップS11）。

【0098】次に、統計処理部222は、第1グループのデータ $A_{min}(i)$ を利用する場合には、各 $W(i)$ について、 $A_{min}(1)$ 、 $A_{min}(2)$ 、…、 $A_{min}(M)$ の平均 $\langle A_{min} \rangle$ を求める（ステップS12）。ただし、それらの値が取りうる最大値と最小値との差（ $=$ 対応する $N(i)$ の値）で除して正規化する。すなわち、 $W(i)$ 、 $N(i)$ 、 $A(i)$ についての第1グループのデータの平均（第1の平均） $\langle A_{min} \rangle$ は、

$$\langle A_{min} \rangle = \{ A_{min}(1) / N(1) + A_{min}(2) / N(2) + \dots + A_{min}(M) / N(M) \} /$$

M

である。

【0099】また、第2グループのデータAmax(i)を利用する場合には、統計処理部222は、各W(i)、N(i)、A(i)についての第2グループのデータの平均(第2の平均)<Amax>を求める(ステップS12)。<Amax>は、  

$$\langle A_{\max} \rangle = \{A_{\max}(1)/N(1) + A_{\max}(2)/N(2) + \dots + A_{\max}(M)/N(M)\} / M$$

である。

【0100】第1グループのデータAmin(i)および第2グループのデータAmax(i)を利用する場合には、<Amin>および<Amax>を求める(ステップS12)。

【0101】次に、推定結託数算出部223は、後述するような方法によって、<Amin>や<Amax>から、結託数の推定値C0を求める(ステップS13)。

【0102】以下、結託数の推定値C0を求める方法について説明する。

【0103】ここで、C0人の結託者による結託攻撃が行われたとする。

【0104】前述したように、このC0が、結託耐性符号の想定している結託数の上限cを越えているか否かを知ることによって、例えば、追跡アルゴリズムが出力した結託者のユーザIDが正しいものであるか、それとも無実のユーザのものであるかに関する判断の材料となる。

【0105】前述したように、各成分符号W(i)において、結託語の符号後を復号することによって、AminやAmaxを検出することができ(それらは、いずれかの結託者の結託前の符号語の対応する成分符号WのAmin=Amaxである)、それらに対して統計的な処理を行うことでC0を推定することができる。統計的な処理の方法は様々あるが、ここでは、各成分符号W(i)についてのAmin(i)の平均<Amin>からC0を推定する方法について説明する。

【0106】ある成分符号W(i)について、各結託者に割り当てられている整数A(i)が0からN(i)-1までの整数のいずれかをとり確率は、0からN(i)-1までの整数のいずれについても等しく、1/N(i)で与えられるとすると、Amin(i)がある値xをとる確率Pr[Amin(i)=x]は、結託者の数がC0のとき、次式で与えられる。

【0107】

【数1】

$$\Pr[A_{\min}(i) = x] = \left(1 - \frac{x}{N(i)}\right)^{C_0} - \left(1 - \frac{x+1}{N(i)}\right)^{C_0}$$

ここで、xは、0からN(i)-1までの整数に値をと

る。

【0108】そこで、実際に復号によって得られた各々の成分符号W(i)についてのAmin(i)を、それぞれ、それらの値が取りうる最大値と最小値との差すなわちN(i)の値で除して正規化し(Amin(i)/N(i))、M個のAmin(i)/N(i)の平均<Amin>、すなわち、

$$\langle A_{\min} \rangle = \{A_{\min}(1)/N(1) + A_{\min}(2)/N(2) + \dots + A_{\min}(M)/N(M)\} / M$$

10 M

を求める。

【0109】<Amin>は、y=x/N(i)を0から1の間の実数として連続近似することによって、次のような期待値<y>で近似できる。

【0110】

【数2】

$$\langle y \rangle = \int_0^1 dy y P(y) = c_0 \int_0^1 dy y (1-y)^{c_0-1} = \frac{1}{c_0 + 1}$$

20 【0111】ここで、P[y]は、Pr[Amin(i)=x]に対するN(i)→∞の連続極限によって与えられ、次式で表される。

【0112】

【数3】

$$P(y) = \lim_{N(i) \rightarrow \infty} N(i) \Pr[\min = N(i)y] = c_0 (1-y)^{c_0-1}$$

【0113】よって、<Amin>=<y>の近似より、C0=<Amin><sup>-1</sup>-1となり、結託数C0が推定できる。

30

【0114】<Amax>を用いた場合にも、同様にして、C0=(1-<Amax>)<sup>-1</sup>-1となり、結託数C0が推定できる。

【0115】また、<Amin>および<Amax>を用いて、C0=(1/2+<Amin>/2-<Amax>/2)<sup>-1</sup>-1として、結託数C0を推定することもできる。

【0116】したがって、第1グループのデータAmin(i)のみを利用する場合には、推定結託数算出部223は、上記のような方法によって、<Amin>から、結託数の推定値C0を求めることができる。

【0117】また、第2グループのデータAmax(i)のみを利用する場合には、推定結託数算出部223は、上記のような方法によって、<Amax>から、結託数の推定値C0を求めることができる。

【0118】また、第1グループのデータAmin(i)および第2グループのデータAmax(i)を利用する場合には、推定結託数算出部223は、上記のような方法によって、<Amin>および<Amax>から、結託数の推定値C0を求める。

50

31

【0119】なお、第1グループのデータ  $A_{min}$  (i) および第2のグループのデータ  $A_{max}$  (i) を利用する場合には、推定結託数算出部223は、 $\langle A_{min} \rangle$  から、結託数の推定値  $C0$  ( $C_{min}$  とする) を求めるとともに、 $\langle A_{max} \rangle$  から、結託数の推定値  $C0$  ( $C_{max}$  とする) を求め、 $C_{min}$  と  $C_{max}$  を列記して出力するか、または  $C_{min}$  と  $C_{max}$  のうちの最大値を出力するか、または  $C_{min}$  と  $C_{max}$  の平均を出力することも可能である (その他のバリエーションも可能である)。

【0120】ここで、具体例を示す。ここでは、 $M=2 \times 10$  粋して示すと、次のようになった。

W(1)	:	N(1)=512、 $A_{min}=13$ 、 $A_{max}=497$
W(2)	:	N(2)=513、 $A_{min}=46$ 、 $A_{max}=505$
W(3)	:	N(3)=515、 $A_{min}=16$ 、 $A_{max}=500$
W(4)	:	N(4)=517、 $A_{min}=7$ 、 $A_{max}=507$
W(5)	:	N(5)=521、 $A_{min}=19$ 、 $A_{max}=519$
W(6)	:	N(6)=523、 $A_{min}=24$ 、 $A_{max}=451$
W(7)	:	N(7)=527、 $A_{min}=123$ 、 $A_{max}=474$
W(8)	:	N(8)=529、 $A_{min}=54$ 、 $A_{max}=524$
W(9)	:	N(9)=533、 $A_{min}=19$ 、 $A_{max}=478$
W(10)	:	N(10)=541、 $A_{min}=4$ 、 $A_{max}=530$
:	:	:
W(247)	:	N(257)=2239、 $A_{min}=31$ 、 $A_{max}=2172$
W(248)	:	N(248)=2243、 $A_{min}=229$ 、 $A_{max}=2142$
W(249)	:	N(249)=2251、 $A_{min}=197$ 、 $A_{max}=2029$
W(250)	:	N(250)=2267、 $A_{min}=133$ 、 $A_{max}=2167$
W(251)	:	N(251)=2269、 $A_{min}=125$ 、 $A_{max}=2033$
W(252)	:	N(252)=2273、 $A_{min}=84$ 、 $A_{max}=2260$
W(253)	:	N(253)=2281、 $A_{min}=55$ 、 $A_{max}=2192$
W(254)	:	N(254)=2287、 $A_{min}=53$ 、 $A_{max}=2164$
W(255)	:	N(255)=2293、 $A_{min}=29$ 、 $A_{max}=2209$
W(256)	:	N(256)=2297、 $A_{min}=13$ 、 $A_{max}=2207$

また、256個の  $A_{min}$  から  $\langle A_{min} \rangle$  を計算すると、

$$\langle A_{min} \rangle = 0.061871$$

が得られ、これを、 $C0 = \langle A_{min} \rangle - 1 - 1$  に代入することによって、

$$C0 = 15.163 \text{ (人)}$$

となり、真の結託者の数に近い値が得られた。

【0121】また、 $\langle A_{max} \rangle = 0.93538$  が得られ、これを、 $C0 = (1 - \langle A_{max} \rangle) - 1 - 1$  に代入することによって、

$$C0 = 14.475 \text{ (人)}$$

となり、真の結託者の数に近い値が得られていることがわかる。

【0122】また、 $C0 = (1/2 + \langle A_{min} \rangle / 2 - \langle A_{max} \rangle / 2) - 1 - 1$  を用いると、

$$C0 = 14.811 \text{ (人)}$$

となり、真の結託者の数に近い値が得られていることがわかる。

【0123】同様の条件で、ある32人の結託攻撃を行

32

\*56、 $N(1)=512$ 、 $N(256)=2297$ 、 $N(2) \sim N(255)$  は513から2293の間の値とし、 $d=30$  の  $\Gamma_0(n, d)$  符号を用いることとして、ある16人で結託攻撃を行った場合に、結託攻撃後のコンテンツから検出した符号 (ユーザ識別符号) をもとに、256個の成分符号  $W(1) \sim W(256)$  について、 $A_{min}(1)$ 、 $A_{max}(1)$ 、 $A_{min}(2)$ 、 $A_{max}(2)$ 、…、 $A_{min}(256)$ 、 $A_{max}(256)$  を求めた一例において、その一部を抜

粋して示すと、次のようになった。

った場合における、結託数の推定結果の一例は、次のようになった。

$$\langle A_{min} \rangle = 0.029065$$

$$\langle A_{max} \rangle = 0.966843$$

$$C0 = \langle A_{min} \rangle - 1 - 1 = 33.406$$

$$C0 = (1 - \langle A_{max} \rangle) - 1 - 1 = 29.160$$

$$C0 = (1/2 + \langle A_{min} \rangle / 2 - \langle A_{max} \rangle / 2) - 1 - 1 = 31.143$$

同様の条件で、ある48人の結託攻撃を行った場合における、結託数の推定結果の一例は、次のようになった。

$$\langle A_{min} \rangle = 0.019884$$

$$\langle A_{max} \rangle = 0.977382$$

$$C0 = \langle A_{min} \rangle - 1 - 1 = 49.292$$

$$C0 = (1 - \langle A_{max} \rangle) - 1 - 1 = 43.213$$

$$C0 = (1/2 + \langle A_{min} \rangle / 2 - \langle A_{max} \rangle / 2) - 1 - 1 = 46.057$$

(バリエーション2) 次に、他のバリエーションを説明する。

【0124】ここでは、バリエーション1との相違点を説明する。バリエーション1では、統計処理部222は、 $A_{min}(i)$  の平均や  $A_{max}(i)$  の平均を求

50

め、推定結託数算出部 223 は、 $A_{min}(i)$  の平均や  $A_{max}(i)$  の平均から、結託者の数  $c_0$  を推定した。

【0125】バリエーション 2 では、統計処理部 222 は、 $A_{min}(i)$  や  $A_{max}(i)$  から、他の統計量を求め、推定結託数算出部 223 は、該他の統計量から、結託者の数  $c_0$  を推定する。

【0126】例えば、図 15 をみると、 $A_{min}(i)$  については、結託数  $c$  が大きくなるほど、横軸におけるある値  $A_{th}$  を基準値として、基準値  $A_{th}$  以下の値を持つ  $A_{min}(i)$  の数を、基準値  $A_{th}$  を越える値を持つ  $A_{min}(i)$  の数で割った比  $\alpha$  が大きくなること

がわかる。一方、 $A_{max}(i)$  については、結託数  $c$  が大きくなるほど、比  $\alpha$  が小さくなる。

【0127】そこで、例えば先の例のように、ある成分符号  $W(i)$  について、各結託者に割り当てられている整数  $A(i)$  が 0 から  $N(i) - 1$  までの整数のいずれかをとり確率は、0 から  $N(i) - 1$  までの整数のいずれについても等しく、 $1/N(i)$  で与えられるとして、予め、結託数  $c$  のときの、基準値  $A_{th}$  以下の値を持つ  $A_{min}(i)$  の数を、基準値  $A_{th}$  を越える値を持つ  $A_{min}(i)$  の数で割った比  $\alpha$  を与える関数  $f(c) = \alpha$  の逆関数  $c = f^{-1}(\alpha)$  を予め求めておく。

【0128】そして、統計処理部 222 は、 $A_{min}(i)$  から、比  $\alpha$  を求め(ステップ S12)、推定結託数算出部 223 は、比  $\alpha$  を、上記の  $c = f^{-1}(\alpha)$  に代入して、結託数  $c$  を推定することができる(ステップ S13)。 $A_{max}(i)$  についても同様である。もちろん、 $A_{min}(i)$  と  $A_{max}(i)$  の一方を用いてもよいし、両方を用いてもよい。

【0129】なお、上記では、結託数の値を推定するようにしたが、結託数を何段階かのレベルで求めるようにしてもよい。例えば、 $A_{min}(i)$  について求めた上記の比  $\alpha$  が予め定められた基準値以下の場合には、結託数が少ない(あるいは許容数以下)を示す情報を出力し、予め定められた基準値を越える場合には、結託数が多い(あるいは許容数を超過)を示す情報を出力する関数を用いるようにしてもよい。

【0130】また、これまで説明した以外のバリエーションも可能である。

【0131】(第 2 の構成例) 次に、図 4 に例示されるような、追跡アルゴリズム処理部 23 の結果を利用して、結託攻撃に使用された複製物の個数を推定する場合(結託数推定部の第 2 の態様の場合)について説明する。なお、前述したように、結託耐性符号や追跡アルゴリズムは、基本的には、どのようなものでも適用可能である。また、結託攻撃がなされなかった場合を、結託攻撃に使用された複製物の個数 = 1 として扱うものとする。

【0132】図 16 に、この場合の結託数推定部 22 の

構成例を示す。図 16 に示されるように、この結託数推定部 22 は、追跡アルゴリズム処理部 23 から結託者の全部または一部のユーザ ID が出力された場合に、該ユーザ ID を後述する弱 ID (弱識別情報) と非弱 ID (非弱識別情報) とに分類する弱 ID・非弱 ID 分類部 241、この分類結果を基に、弱 ID の数と非弱 ID の数とに基づく統計的な量を求める統計処理部 242、求められた統計的な量から結託数の推定値  $C_0$  を求める推定結託数算出部 243 を含む。なお、統計処理部 242 および推定結託数算出部 243 による統計的な処理の方法には種々のバリエーションが考えられる。

【0133】図 17 に、概略的な手順の一例を示す。

【0134】なお、この場合には、電子透かし埋込装置 1 (の符号生成部 11) は、弱 ID をユーザ ID として用いないものとする。

【0135】以下では、第 1 の構成例との相違点を中心に説明する。

【0136】ここで、弱 ID と非弱 ID について説明する。

【0137】弱 ID とは、ユーザ ID として用いた場合に、結託攻撃を行っていないユーザのユーザ ID であるにもかかわらず、結託者のユーザ ID として誤検出される可能性のより高いユーザ ID である(誤検出に弱い ID という意味から、このように呼ぶ)。非弱 ID とは、ユーザ ID 候補のうちから、弱 ID を除いたユーザ ID であり、非弱 ID のみがユーザ ID として使用される。

【0138】非弱 ID は、所定の判定アルゴリズムによって判定する方法と、誤検出される可能性のより高いユーザ ID を何らかの指針(例えば、対応する結託耐性符号の成分符号の全部または多数について、その正規化した  $A_{min} = A_{max}$  が 0 または 1 に近い等)によって予め決めてしまう方法とがある。

【0139】ここで、図 18 に示すフローチャートを用いて、図 7 の符号生成部 11 の場合に、与えられたユーザ ID (の候補) が弱 ID か非弱 ID かを判定する処理手順の一例について説明する。

【0140】まず、対象となったユーザ ID を一つずつシーケンシャルに入力し(ステップ S31)、このユーザ ID が結託者 ID として誤検出される確率(誤検出確率)を推定する(ステップ S32)。この誤検出確率の推定は、例えば前述した  $p_i (= N(i))$ 、 $k$ 、 $k' (= M)$ 、結託者総数の最大値  $c$ 、ユーザ総数  $n$ 、 $z$  といったパラメータを用いて次のようにして行われる。なお、 $k$  については、図 7 の法記憶部 121-1、121-2、 $\dots$ 、121- $k'$  で用意されている  $k'$  個の素数  $p_1 (= N(1))$ 、 $p_2 (= N(2))$ 、 $\dots$ 、 $p_{k'} (= N(k'))$  から任意の  $k$  個の素数を選んだとき、それらの  $k$  個の素数の積を  $n$  以上とするものである(例えば、この積は  $n \leq N(1) \times N(2) \times \dots \times N(k)$  である)。また、 $z$  は、1 以上の正整数であり、例え

35

ば、 $k' = c(k+z)/2$ を満足する正整数である。

【0141】まず、次式を定義する。

$$\Pr[x; p, c] = \begin{cases} \left(1 - \frac{x}{p}\right)^c - \left(1 - \frac{x+1}{p}\right)^c & \text{for } x \neq p-1 \\ \left(\frac{1}{p}\right)^c & \text{for } x = p-1 \end{cases}$$

次に、次式を定義する。

【0143】

【数5】

$$Q[x; p, c] = \Pr[x; p, c] + \Pr[p-1-x; p, c]$$

【0144】あるユーザID(=uとする)が結託者ID※

$$EEP = 1 - \prod_{\{j(1), j(2), \dots, j(k+z)\} \subset \{1, 2, \dots, k'\}, j(1) < j(2) < \dots < j(k+z)} \left\{ 1 - \prod_{j=1, 2, \dots, k+z} Q[u_{p_i}; p_i, c] \right\}$$

【0146】ここで、 $u_p = u \bmod p$ とする。これ以外にも、ある利用者IDについて誤検出確率を近似する評価値が存在するならば、それを該評価値EEPの代わりに用いることが可能である。例えば、次式で表される評価値EEPを用いてもよい。

【0147】

【数7】

$$EEP = \sum_{i=1, 2, \dots, k'} Q[u_{p_i}; p_i, c]$$

【0148】次に、ステップS32で推定された誤検出確率(例えば、該EEP)が所定の閾値を超えたか否かを調べ(ステップS33)、閾値を超える場合は、ユーザID(の候補)が弱IDであると判定し(ステップS34)、また誤検出確率が閾値以下の場合は、ユーザID(の候補)が非弱IDであると判定する(ステップS35)。

【0149】さて、結託攻撃を行った結託数cが大きくなると、追跡アルゴリズムが当該結託攻撃を受けたコンテンツから結託者のユーザIDを推定した場合に、得られる結果として弱IDが増加してくる。したがって、弱IDの数と非弱IDの数との比 $\beta$ を評価することで、その比 $\beta$ を生み出す結託数cの値が推定できる。

【0150】すなわち、結託数cが大きくなるほど、弱IDの数を、非弱IDの数で割った比 $\beta$ が大きくなるので、予め、結託数cのときの比 $\beta$ を与える関数 $h(c) = \beta$ の逆関数 $c = h^{-1}(\beta)$ を予め求めておくことで、比 $\beta$ から結託数cを推定することができる。

【0151】まず、弱ID・非弱ID分類部241は、追跡アルゴリズム処理部23から結託者の全部または一部のユーザIDが出力された場合に、該ユーザIDを、弱IDと非弱IDとに分類する(ステップS21)。なお、弱IDか非弱IDかの判断は、例えば、弱IDのリストを記憶しておき、与えられたユーザIDが該リストに登録されているものと一致するか否かを調べることに

36

\*【0142】

\*【数4】

※として誤検出される確率を概ね表す量として、次式で表される評価値EEPを計算する。

10 【0145】

【数6】

よって、一致すれば弱IDと判断し、一致しなければ非弱IDと判断するようにしてもよいし、ユーザIDが弱IDか非弱IDかを判定する手順が作成可能であれば、該判断手順によって弱IDか非弱IDかを判断するようにしてもよい。

【0152】次に、統計処理部222は、分類された弱IDと非弱IDとに基づいて、弱IDの数を非弱IDの数で割った比 $\beta$ を求める(ステップS22)。

【0153】そして、推定結託数算出部223は、比 $\beta$ を、上記の $c = h^{-1}(\beta)$ に代入して、結託数cを推定することができる(ステップS23)。

【0154】なお、上記では、結託数の値を推定するようにしたが、結託数を何段階かのレベルで求めるようにしてもよい。例えば、求めた上記の比 $\beta$ が予め定められた基準値以下の場合には、結託数が少ない(あるいは許容数以下)を示す情報を出力し、予め定められた基準値を超える場合には、結託数が多い(あるいは許容数を超過)を示す情報を出力する関数を用いるようにしてもよい。

【0155】なお、以上では、コンテンツの複製物に、ユーザIDに対応する符号を埋め込むようにしたが、その代わりに、複製物の複製物IDとそのユーザを特定するための情報(例えば、ユーザ名、あるいはユーザID等)との対応を保存または復元可能にしておき、コンテンツの複製物に、複製物IDに対応する符号を埋め込むようにしてもよい。

【0156】以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【0157】本実施形態の電子透かし解析装置は、ハードウェアとしても、ソフトウェア(コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための)プログラムとしても、実現可能である。また、電子透かし解析装置を

50

37

ソフトウェアで実現する場合には、記録媒体によってプログラムを受け渡すことも、通信媒体によってプログラムを受け渡すこともできる。もちろん、それらは、電子透かし埋込装置についても同様である。また、電子透かし埋込装置や電子透かし解析装置をハードウェアとして構成する場合、半導体装置として形成することができる。また、本発明を適用した電子透かし解析装置を構成する場合、あるいは電子透かし解析プログラムを作成する場合に、同一構成を有するブロックもしくはモジュールがあっても、それらをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては1または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。電子透かし埋込装置を構成する場合、あるいは電子透かし埋め込みプログラムを作成する場合も、同様である。また、電子透かし埋込装置および電子透かし解析装置を含むシステムを構成する場合、あるいは電子透かし埋め込みプログラムおよび電子透かし検出プログラムを含むシステムを作成する場合には、電子透かし埋込装置（あるいはプログラム）と電子透かし解析装置（あるいはプログラム）に渡って、同一構成を有するブロックもしくはモジュールについては1または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【0158】また、電子透かし埋込装置や電子透かし解析装置をソフトウェアで構成する場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【0159】ところで、デジタル透かしに対する透かし技術は、デジタルデータの他に、ある情報あるいは物質の一部の内容を変更しても、その情報あるいは物質の同一性、同質性あるいは経済的価値等を変じないようなものにも適用可能であり、本発明は、デジタルデータの他に、そのような情報あるいは物質にも適用可能である。

【0160】例えば、本発明において、結託攻撃への耐性を持つ電子透かし埋込装置／電子透かし解析装置において用いられる、埋め込まれる符号の生成手段、検出手段は、化学的に合成される、あるいは、工業的に管理された環境下で生物的に生成される化合物あるいは化学物質の出所の追跡にも応用できる。化合物としては、DNA、RNA、タンパク質、その他の高分子の化合物が、符号を埋め込むことができる冗長性を多く持つ。

【0161】以下では、本発明を、化合物の複製物に対して個別の識別情報（ユーザID、製造者ID、販売者ID、取引ID、それらを組み合わせた情報など）を埋め込み、その出所を特定する手段を与える透かし技術として適用する場合について説明する。

【0162】化合物は、複数の原子、分子、基といった物質から構成されている。例えば、DNAやRNAは、所定のアミノ酸の配列構造を持っており、別のアミノ酸

38

で置きかえるか如何かによって情報が表現されているとみなせる。その構造の中には、（デジタルコンテンツの場合には、データを変更しても、作品の同一性あるいは経済的価値を変えない場合があるのと同様に、）化合物の場合には、組成を変更しても、当該目的において、その作用・副作用・効用等の性質・機能等（別の観点で見れば、経済的価値）を変えない場合がある。

【0163】そのような許容された範囲内の変更によって、その複製物を個々に識別する情報を埋め込むことができる。

【0164】本発明の電子透かしを化合物に適用する場合、化合物に対する透かし埋込装置は、デジタルコンテンツに対する透かし埋込装置におけるデジタルコンテンツの所定の部分のビットを変更する構成を、化合物の所定の部分の組成を変更する装置に置き換えたものである。また、化合物に対する透かし解析装置は、デジタルコンテンツに対する透かし解析装置において透かし情報を検出するためにデジタルコンテンツの所定の部分のビットの値を読み取る情報を検出する構成を、透かし情報を検出するために化合物の所定の部分の組成を解析する装置に置き換えたものである。すなわち、化合物とのインタフェースとなる装置が相違するだけで、原理的には、デジタルコンテンツに対する透かし技術と同じである。

【0165】図19に、化合物に対する透かし埋込装置の構成例を示す。

【0166】符号生成部1001は、その化合物に埋め込むべき識別情報を入力とし、結託耐性符号を生成する。

【0167】特定部位の構造変換部1002～1004は、それぞれ、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じて化合物の構造を変換するものである。特定部位の構造変換部1002は、原化合物の特定部位1を処理し、特定部位の構造変換部1003は、特定部位1を処理済みの化合物の特定部位2を処理し、特定部位の構造変換部1004は、特定部位1、2を処理済みの化合物の特定部位3を処理して、所望する埋込済み化合物を生成する。もちろん、図19では、3つの構造変換部が示されているが、その数は3に限定されるものではない。

【0168】ここで、化合物の構造の変換とは、その化合物の利用の目的に適した性質あるいは機能等を損なわず且つ新たな弊害あるいは副作用等をもたらさないままで、異なる構造を持つ化合物に変換する手段のことである。あるいは、その化合物が純粋な化合物ではなく、混合物である場合には、その組成を変更する手段であってもよい。

【0169】図20に、化合物に対する透かし埋込装置の他の構成例を示す。

【0170】図19の構成例は、すでに合成された化合

39

物の構造を後から変換するものであったが、図 20 の構成例は、化合物の合成時に符号を埋め込むものである。

【0171】符号生成部 1011 は、その化合物に埋め込むべき識別情報を入力とし、結託耐性符号を生成する。

【0172】この場合、各合成材料毎に、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じた合成材料が容易されており、合成材料部 1012~1014 は、それぞれ、結託耐性符号の各ビット、あるいは、ビットの各集合に対して、その値に応じた化合物の合成材料を選択するものである。もちろん、図 20 では、3 つの合成材料選択部が示されているが、その数は 3 に限定されるものではない。

【0173】合成部 1015 は、各合成材料部 1012~1014 により選択された合成材料を合成して、所望する埋込済み化合物を生成する。

【0174】さて、化合物に対する結託攻撃では、基本的にはデジタルコンテンツに対する結託攻撃と同様で、例えば、複数の異なる識別情報（例えば、ユーザ ID、製造者 ID、ユーザ ID 及び製造者 ID 等）が埋め込まれた化合物の構造を比較することで、差異のある部分の構造を改変することで作られる。

【0175】図 21 に、化合物に対する透かし解析装置の構成例を示す。

【0176】特定部位の構造読み取り部 1201~1201 は、図 19 の特定部位の構造変換部 1002~1004 あるいは図 20 の合成材料部 1012~1014 に対応するもので、その化合物中の特定部位の構造を読み取り、それをビットあるいはビットの集合である情報として出力する。

【0177】符号復号部 1204 は、それらのビットから追跡すべき符号語を再現し、結託数を推定するもので、デジタルコンテンツに対する電子透かし解析装置 2 の持つ、ビットから追跡すべき符号語を再現し、結託数を推定する機能と同様である。

【0178】もちろん、化合物に対する透かし解析装置は、必要に応じて、追跡アルゴリズムの機能を持つものである。

【0179】また、化合物に対する透かし解析装置は、結託数を推定する機能を持たず、追跡アルゴリズムの機能を持つ構成も可能である。

【0180】ここで、本発明に用いられる化合物の構造の変換手段や構造の読み取り手段について、利用可能な技術を例示する。以下では、DNA の場合を例にとって説明する。

【0181】DNA において、その塩基配列を求めることを、シーケンシングという。シーケンシングの方法としては、ショットガン法、プライマーウォーク法、ネステッドデレクション法などが知られている。これ

40

らは、いずれも遺伝子のクローニングによる方法である。シーケンシングで用いる試薬・機器・装置の例については、各種の方法が提案されている。例えば、渡辺格監修、杉浦昌弘編集「クローニングとシーケンス」、農村文化社（1989 年）や、榊佳之等編「ゲノムサイエンス」、共立出版（1999 年）などに開示されている。

【0182】同様に、DNA の例では、新しい遺伝子を導入する際に用いられている遺伝子導入法により構造変換が可能である。遺伝子導入法には、燐酸カルシウム沈殿法、デキストラン法、リポフェクション法などの化学的な方法や、電気穿孔法、マイクロインジェクション法などが知られている。例えば、波賀信幸著「分子細胞工学」、コロナ社（2000 年）に開示されている。

【0183】なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、この発明の実施の形態は、個別装置としての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【0184】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0185】

【発明の効果】本発明によれば、結託耐性符号の埋め込まれたデジタルコンテンツの複製物から検出した符号についての統計的な手法に基づく推定を行うことによって、結託攻撃に用いられたデジタルコンテンツの複製物の数を推定することができる。

【図面の簡単な説明】

【図 1】本発明の一実施形態に係る電子透かし埋込装置及び電子透かし解析装置を含むコンテンツ流通システムの概略構成を示す図

【図 2】同実施形態に係る電子透かし埋込装置の構成例を示す図

41

【図3】同実施形態に係る電子透かし解析装置の構成例を示す図

【図4】同実施形態に係る電子透かし解析装置の他の構成例を示す図

【図5】同実施形態に係る電子透かし解析装置のさらに他の構成例を示す図

【図6】同実施形態に係る電子透かし埋込装置の概略的な手順の一例を示すフローチャート

【図7】同実施形態に係る電子透かし埋込装置の符号生成部の構成例を示す図

【図8】図7の符号生成部の成分符号生成部の構成例を示す図

【図9】同実施形態に係る電子透かし埋込装置により生成される成分符号の例について説明するための図

【図10】同実施形態における各ユーザIDに対応する複数の整数の組の例について説明するための図

【図11】同実施形態における各ユーザIDに対応する結託耐性符号の例について説明するための図

【図12】同実施形態における各成分符号でのビットパターンに関する境界の位置について説明するための図

【図13】同実施形態に係る電子透かし解析装置の結託数推定部の構成例を示す図

【図14】同実施形態に係る電子透かし解析装置の結託数推定部の概略的な手順の一例を示すフローチャート

【図15】結託攻撃において用いる複製物の個数と、改ざんされた結託耐性符号の各成分符号において検出されるビットパターンに関する境界の位置との関係について説明するための図

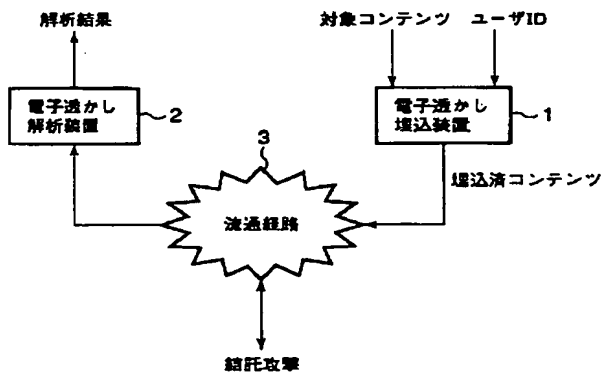
【図16】同実施形態に係る電子透かし解析装置の結託数推定部の他の構成例を示す図

【図17】同実施形態に係る電子透かし解析装置の結託数推定部の概略的な手順の他の例を示すフローチャート

【図18】同実施形態においてユーザIDが弱IDか非弱IDかを判定するための手順の一例を示すフローチャート

【図19】同実施形態に係る化合物に対する透かし埋込\*

【図1】



42

\*装置の構成例を示す図

【図20】同実施形態に係る化合物に対する透かし埋込装置の他の構成例を示す図

【図21】同実施形態に係る化合物に対する透かし解析装置の他の構成例を示す図

【符号の説明】

1…電子透かし埋込装置

2…電子透かし解析装置

3…流通経路

10 1 1…符号生成部

1 2…符号埋込部

2 1…符号抽出部

2 2…結託数推定部

2 3…追跡アルゴリズム処理部

1 2 1-1~1 2 1-k'…法記憶部

1 2 2-1~1 2 2-k'…剰余計算部

1 2 3…符号パラメータ記憶部

1 2 4-1~1 2 4-k'…成分符号生成部

1 2 5…符号接続部

20 1 3 1…減算部

1 3 2…“0”列生成部

1 3 3…“1”列生成部

3 4…接続部

2 2 1…境界検出部

2 2 2…統計処理部

2 2 3…推定結託数算出部

2 4 1…弱ID・非弱ID分類部

2 4 2…統計処理部

2 4 3…推定結託数算出部

30 1 0 0 1, 1 0 1 1…符号生成部

1 0 0 2~1 0 0 4…特定部位の構造変換部

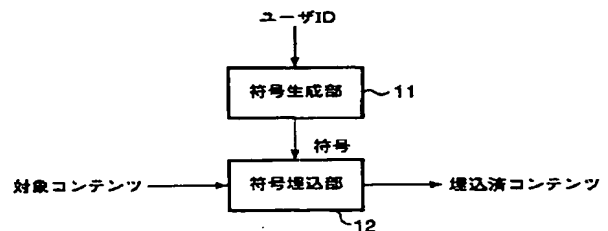
1 0 1 2~1 0 1 4…合成材料部

1 0 1 5…合成部

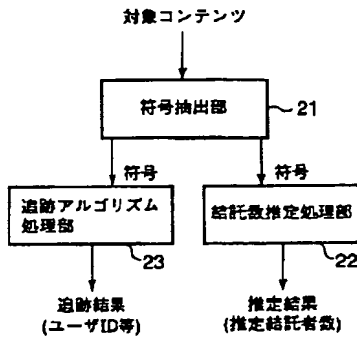
1 2 0 1~1 2 0 1…特定部位の構造読み取り部

1 2 0 4…符号復号部

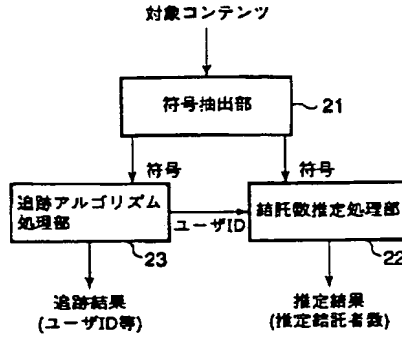
【図2】



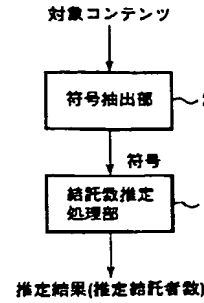
【図3】



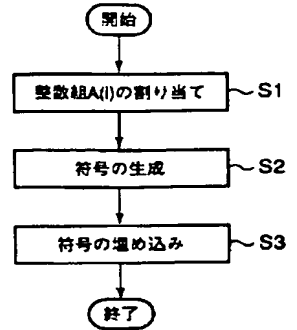
【図4】



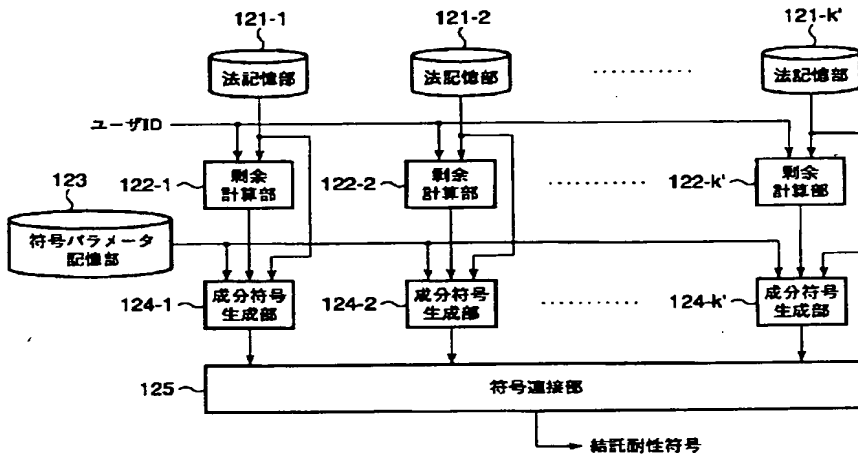
【図5】



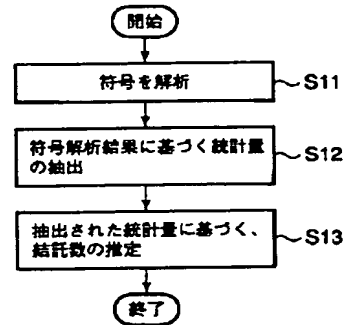
【図6】



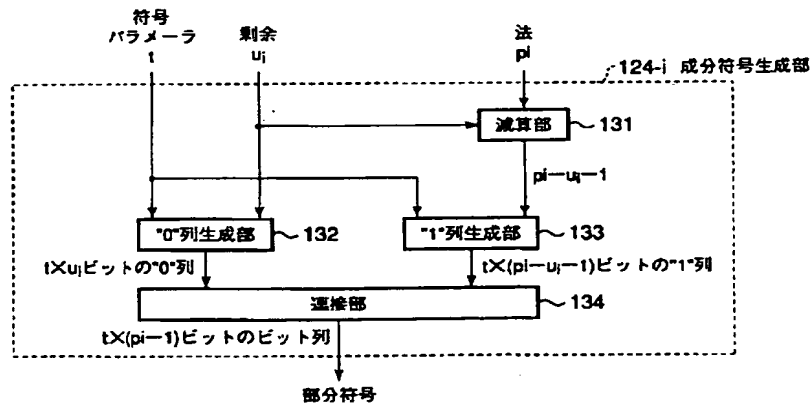
【図7】



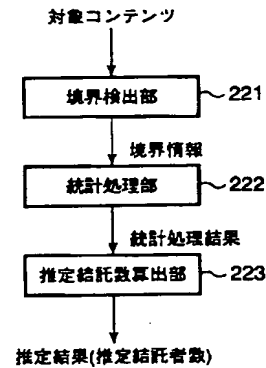
【図14】



【図8】



【図13】



【図9】

ユーザID	B(0)	B(1)	...	B(Smin)	...	B(Smax)	...	B(n-3)	B(n-2)
0	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1
1	0...0	1...1	1...1	1...1	1...1	1...1	1...1	1...1	1...1
...									
Smin	0...0	0...0	0...0	1...1	1...1	1...1	1...1	1...1	1...1
...									
Smax	0...0	0...0	0...0	0...0	0...0	1...1	1...1	1...1	1...1
...									
n-2	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0	1...1
n-1	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0	0...0

【図10】

ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A(1)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
A(2)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
A(3)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

【図12】

	符号	B(0)	B(1)	B(2)	...	B(N-3)	B(N-2)	
(a)	:	:	:	:	:	:	:	:
Amin	→	0	1	2	3	N-3	N-2	N-1
		0	1	2	3	N-3	N-2	N-1 ← Amax

	符号	000	000	101	011	111	111	...	111
(b)	:	:	:	:	:	:	:	:	:
Amin	→	0	1	2	3	4	5	6	N-2
		0	1	2	3	4	5	6	N-2
									N-1 ← Amax

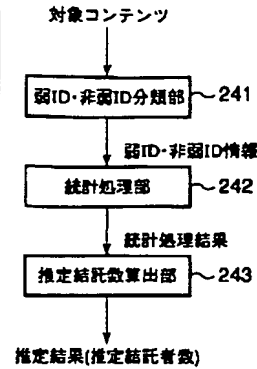
  

	符号	000	000	111	111	111	111	...	111
(c)	:	:	:	:	:	:	:	:	:
Amin	→	0	1	2	3	4	5	6	N-2
		0	1	2	3	4	5	6	N-2
									N-1 ← Amax

	符号	000	000	000	000	111	111	...	111
(d)	:	:	:	:	:	:	:	:	:
Amin	→	0	1	2	3	4	5	6	N-2
		0	1	2	3	4	5	6	N-2
									N-1 ← Amax

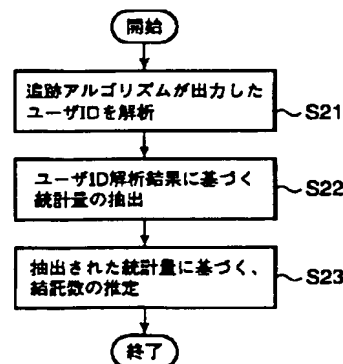
【図16】



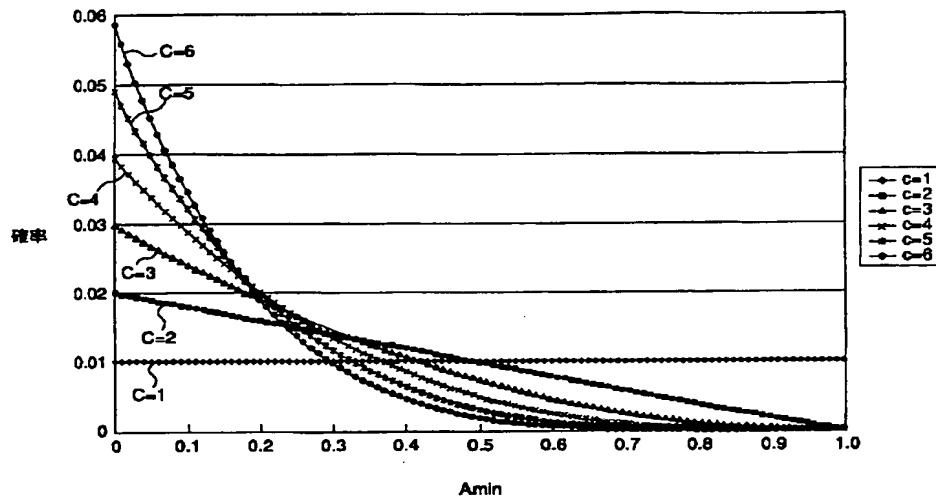
【図11】

ID	IDに対応する符号(W(1)+W(2)+W(3))		
0	111111	1111111111111111	11111111111111111111
1	000111	0001111111111111	00011111111111111111
2	000000	0000001111111111	00000011111111111111
3	111111	0000000001111111	00000000011111111111
4	000111	0000000000000000	00000000000001111111
5	000000	1111111111111111	00000000000000011111
6	111111	0001111111111111	00000000000000000000
7	000111	0000001111111111	11111111111111111111
8	000000	0000000001111111	00011111111111111111
9	111111	0000000000000000	00000011111111111111
10	000111	1111111111111111	00000000011111111111
11	000000	0001111111111111	00000000000001111111
12	111111	0000001111111111	00000000000000011111
13	000111	0000000001111111	00000000000000000000
14	000000	0000000000000000	11111111111111111111

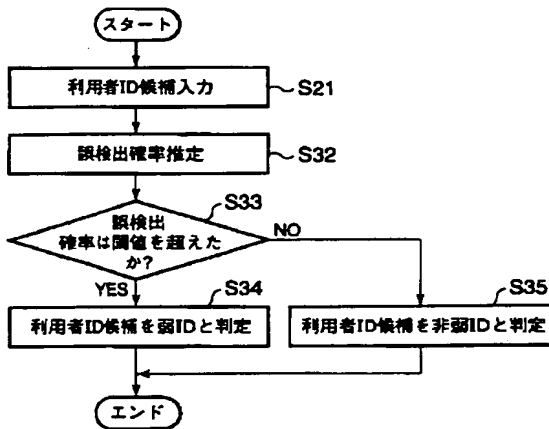
【図17】



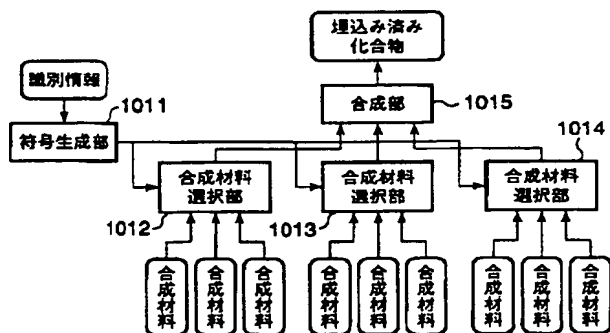
【図15】



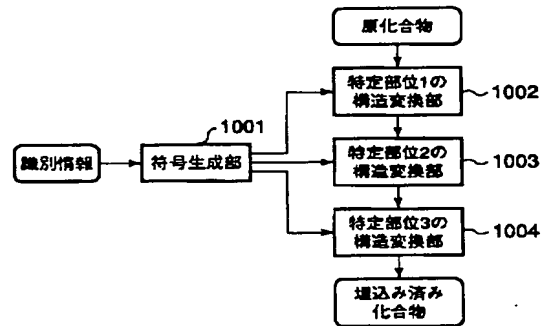
【図18】



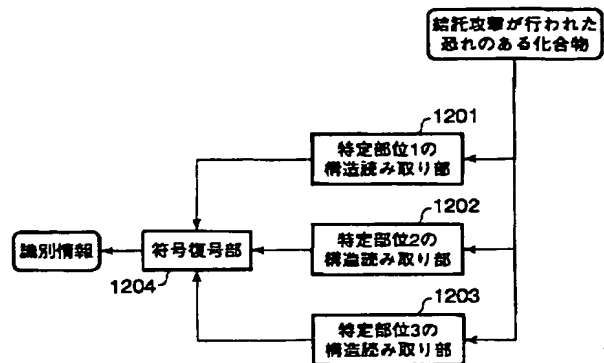
【図20】



【図19】



【図21】



フロントページの続き

(51)Int. Cl. 7

H 0 4 N 7/081

識別記号

F I

テーマコード(参考)